# Upper bound for the $\gcd(u-1, v-1)$, $u,v$ $S$-units, generalisations [generalizations] and applications (Analytic number theory and related topics)

AUTHOR(S):

Corvaja, Pietro

数理解析研究所講究録
第1710巻 2010年 1-6



# Upper bound for the $\gcd(u-1, v-1)$, $u, v$ $S$-units, generalisations and applications

Pietro Corvaja

The goal of this lecture is two-fold: first, it aims at presenting some arithmetic results related to the title of the talk, obtained in the last six years in collaboration with U. Zannier and showing its relation with the so-called Erdös' support problem; second, it makes a connection with an apparently unrelated theory, arising from complex analysis, recently developped by Noguchi, Winkelmann and Yamanoi. Finally, we refer to Noguchi's lecture for the most recent developments in the complex analytic case, obtained by joining ideas from both fields.

## 1 Divisibility between values of power sums

Given two positive integers $a$ and $b$, one expects that the ratio $\frac{b^n-1}{a^n-1}$ will not be an integer for large values of $n$, unless $b$ is a power of $a$, in which case $a^n-1$ divides $b^n-1$ for all integers $n$.

A theorem of van der Poorten [9] (holding actually in greater generality) ensures that if the ratio $\frac{b^n-1}{a^n-1}$ is an integer *for all* integral exponents $n>0$, then $b$ is a power of $a$. A stronger finiteness result was proved by Zannier and the author at the end of last century [5]:

**Theorem 1** *Let $b>a>1$ be integers, $b$ not a power of $a$. Then there exists a number $n_0=n_0(a,b)$ such that for all $n>n_0$, the ratio $\frac{b^n-1}{a^n-1}$ is not an integer.*

So, for instance, $2^n-1$ divides $3^n-1$ only for a finitely many exponents $n$. The method of proof of Theorem 1, which rests on Schmdit's Subspace Theorem, is ineffective, so it does not lead to the determination of the number $n_0(a,b)$ in terms of $a, b$. For instance, it is still unknown for which exponents $n$ does $2^n-1$ divide $3^n-1$.

A natural quantitative problem arises from the finiteness statement of Theorem 1; namely, once we know that the denominator in the fraction $\frac{b^n-1}{a^n-1}$ does not simplify completely, we can try to bound the maximal possible simplification, represented by

the greatest common divisor of $b^n - 1, a^n - 1$. Clearly, if $a, b$ are multiplicatively dependent, i.e. satisfy a relation of the form $a^r = b^s$ for integers $(r, s) \neq (0, 0)$ (and in this case we could then take $r > 0, s > 0$, in view of the hypotheses $a > 1, b > 1$), one can write $a = c^s, b = a^r$ for some integer $c > 1$ so $c^n - 1$ divides both $a^n - 1$ and $b^n - 1$, for every $n$. If, otherwise, no multiplicative relation links $a$ and $b$, it is natural to expect that the $\gcd(a^n - 1, b^n - 1)$ be (logarithmically) infinitesimal with respect to $a^n, b^n$. This became a theorem in 2003, due to Bugeaud, Corvaja, Zannier:

**Theorem 2** *Let $a, b > 1$ be multiplicatively independent integers, $\epsilon > 0$ be a positive real number. Then, provided $n$ is sufficiently large,*

$$\gcd(a^n - 1, b^n - 1) < \exp(\epsilon n).$$

In the above theorem, the terms $a^n, b^n$ can be replaced by element of any finitely generated multiplicative group, up to formulating the inequality in terms of heights. For this reason, we recall the notion of Weil height. Let $k$ be a number field; for $x \in k^*$, its (logarithmic) height $h(x)$ si defined by

$$h(x) = \sum_v \max\{0, \log |x|_v\},$$

where the sum is taken over the normalized absolute values of $k$. This means that the product formula $\prod_v |x|_v = 1$ holds "without weights".

In [7] we proved

**Theorem 3** *Let $k$ be a number field, $\Gamma \subset k^*$ a finitely generated multiplicative group. For multiplicatively independent pairs $(u, v) \in \Gamma \times \Gamma$, the height of the ratio $(u-1)/(v-1)$ satisfies the asymptotic equivalence*

$$h((u - 1)/(v - 1)) \sim \max\{h(u), h(v)\}.$$

Note that for $u = a^n, v = b^n$, the height $h((u - 1)/(v - 1))$ is equal to the maximum between the numerator and the denominator in the *reduced form* of the above fraction; so, in our case, $h((a^n - 1)/(b^n - 1)) = \max(a^n - 1, b^n - 1)/\gcd(a^n - 1, b^n - 1)$. Hence Theorem 3 is a generalizes Theorem 2.

The above statement formally implies a further generalisation , where $u - 1, v - 1$ are replaced by $u - p, u - q$ for arbitrary (but fixed) points $p, q \in k^*$: simply enlarge $\Gamma$ by adjoining $p, q$ and then replace $(u, v)$ by $(u/p, v/q)$.

Theorem 3 applies in particular to questions of divisibility between numbers of the form $a^m - 1, b^n - 1$. It is easy to see that for positive integers $a, b$, with $\gcd(a-1, b) = 1$ there exist infinitely many pairs of integers $(m, n)$ such that $a^m - 1$ divides $b^n - 1$; simply, take any $m \geq 1$ such that $\gcd(a^m - 1, b) = 1$ (there exist infinitely many of them); then take for $n$ the order of $b$ modulo $a^m - 1$ and we are done. With this construction, however, the order of magnitude of $n$ will be larger then that of $m$. As a consequence of the above theorem, we can prove that this will always be the case:

**Corollary 1** *Let $1 < a < b$ be multiplicative independent positive integers. Then the pairs $(m, n)$ for which*

$$\frac{b^n - 1}{a^m - 1} \in \mathbb{Z}$$

*satisfy $n/m \to \infty$.*

A natural generalisation of Theorem 1 concerns divisibility between values of *power sums*; namely, one could replace the two functions $n \mapsto a^n - 1$ and $n \mapsto b^n - 1$ by a pair of functions of the form $n \mapsto b_1 a_1^n + \ldots + b_k a_k^n$, for suitable rational numbers $b_1, \ldots, b_k$ and pairwise distinct positive integers $a_1, \ldots, a_k$. In that case one expects that the divisibility between the values of two such functions holds only for finitely many integers $n$, apart trivial cases, when divisibility holds identically (as in examples like $(4^n - 1)/(2^n - 1)$, where the ratio is always an integer, equal to $2^n + 1$). This was proved in [5]. Actually, the most general case is constituted by the so called *linear recurrence sequences*, i.e. sequences of complex numbers of the form

$$n \mapsto \mathbf{f}(n) := p_1(n)\alpha_1^n + \ldots + p_k(n)\alpha_k^n.$$

Here $\alpha_1, \ldots, \alpha_k$, called the *roots* of $\mathbf{f}$, are pairwise distinct non-zero complex numbers and $p_1(X), \ldots, p_k(X) \in \mathbb{C}[X]$ are polynomials. For simplicity, we shall restrict our attention to the case where the $p_i$ are all constant; in that case the sequence $n \mapsto \mathbf{f}(n)$ will be called a power sum. One of our results in [6] states the following

**Theorem 4** *Let $R \subset \mathbb{C}$ be a subring, finitely generated over the integers. Let $\mathbf{f}_1, \mathbf{f}_2$ be power sums whose roots generate together a torsion-free multiplicative subgroup of $\mathbb{C}^*$. If the ratio $\mathbf{f}_1(n)/\mathbf{f}_2(n)$ belongs to $R$ for infinitely many integers $n$, then the function $n \to \mathbf{f}_1(n)/\mathbf{f}_2(n)$ is a power sum.*

Some remarks: (1) The constraint that the multiplicative group generated by the roots of $\mathbf{f}_1, \mathbf{f}_2$ has no torsion can be avoided (at the cost of slightly rephrasing the conclusion); actually, if $q$ is the order of the torsion sub-group, for every $r = 0, \ldots, q-1$, the power sums $n \mapsto \mathbf{f}_i(qn + r)$ have roots in a torsion-free group; then one can apply the above theorem to the ratios $\mathbf{f}_1(qn + r)/\mathbf{f}_2(qn + r)$, for each value of $r$. (2) The above general result is reduced to the number-field case after applying a standard specialization argument; hence, the most interesting case arises where the roots $\alpha_i$ and coefficients $p_i$ are algebraic numbers and $R$ is a ring of $S$-integers in a number field. (3) In the case $\mathbf{f}_1(n) = b^n - 1$, $\mathbf{f}_2(n) = a^n - 1$, the ratio $\mathbf{f}_1/\mathbf{f}_2$ is a power sum if and only if $b$ is a power of $a$. Hence we re-obtain Theorem 1.

## 2 Support problem

A question closely related to the divisibility problems treated so far was posed by Erdös in 1988: do the prime divisors of $a^n - 1$ determine the positive integer $a$? More generally, if for two fixed positive numbers $a, b$ and all the exponents $n$, the prime divisors of $a^n - 1$ also divide $b^n - 1$, is it true that $b$ is a power of $a$? A positive answer

can be easily deduced from a theorem of Schinzel [10], published already in the sixties, much earlier than Erdös' formulation. An explicit solution, together with its elliptic version, was provided by Corrales-Rodrigañez and Schoof [3] in 1997.

A related problem has been raised by Ailon and Rudnick [1]: let $a$ and $b$ be multiplicatively independent positive inetgers; does the ratio

$$\frac{\gcd(a^n-1, b^n-1)}{\gcd(a-1, b-1)}$$

take the value 1 infinitely often?

In other words, the *supports* of $a^n-1$ and $b^n-1$ should remain as disjoint as possible, for infinitely many $n$.

Let us now see the elliptic curves case; here are two results in the elliptic case, the first one due to Corrales-Rodrigañez and Schoof, the second to Larsen [8]:

**Theorem 5** *Let $E$ be an elliptic curve defined over the ring of $S$-integers in a number field $k$, with origin $O$; let $P_1, P_2 \in E(k)$ be rational points of infinite order. Suppose that for every $n$, the set of primes $\mathcal{P} \in \mathrm{spec}(\mathcal{O}_S)$ such that $nP_1 \equiv 0 \pmod{\mathcal{P}}$ is contained in the set of primes $\mathcal{P}$ such that $nP_2 \equiv 0 \pmod{\mathcal{P}}$. Then there exists an isogeny $\Phi : E \to E$ with $\Phi(P_1) = P_2$.*

**Theorem 6** *Let $E_1, E_2$ be elliptic curves over a ring of $S$-integers, with origins $O_1, O_2$ respectively. Let $P_i \in E(k)$ be non-trosion points. Suppose that for every $n$, the set of primes $\mathcal{P} \in \mathrm{spec}(\mathcal{O}_S)$ such that $nP_1 \equiv 0_1 \pmod{\mathcal{P}}$ is contained in the set of primes $\mathcal{P}$ such that $nP_2 \equiv 0_2 \pmod{\mathcal{P}}$. Then $E_1, E_2$ are $k$-isogenous.*

In both the original (toric) and the elliptic versions, it is essential that one considers the reduction (modulo primes) to the origin of the group. For instance, the Schinzel-Corrales-Schoof-Larsen method of proof does not apply to prime divisors of $a^n - p$, $b^n - q$ for arbitrary $p, q$; to our knowledge, it cannot be escluded that for some choice of $a, b$, the prime divisors of, say, $a^n - 2$ and $b^n - 3$ are the same for all large $n$.

# 3 Geometric formulation

Let us consider again Theorems 1, 4, and rephrase them in more geometric terms. Take a power sum, given by an expression of the form

$$\mathbf{f}(n) = p_1\alpha_1^n + \ldots + p_k\alpha_k^n,$$

where to simplify we suppose that the roots $\alpha_1, \ldots, \alpha_k$ generate a torsion-free multiplicative group in $k^*$, $k$ being a number field, and the coefficients are algebraic numbers in $k$. Then we can take a basis $u_1, \ldots, u_r$ of the group generated by $\alpha_1, \ldots, \alpha_k$ and write $\mathbf{f}(n)$ as a Laurent polynomial in $(u_1^n, \ldots, u_r^n)$ as

$$\mathbf{f}(n) = F(u_1^n, \ldots, u_r^n).$$

Taking a finite set of places $S$ such that $u_1, \ldots, u_r \in \mathcal{O}_S^*$, one can view the point $(u_1, \ldots, u_r) \in \mathcal{O}_S^{*r}$ as an $S$-integral point in the torus $\mathbb{G}_m^r$. Let us denote by $g$ this point, and view it as a morphism $g : spec\, \mathcal{O}_S \to \mathbb{G}_m^r$. Consequently, $g^n$ will be the point $(u_1^n, \ldots, u_r^n)$. Now, let $D$ be the hypersurface defined by $F(X_1, \ldots, X_r) = 0$ in $\mathbb{G}_m^r$. Then the values $\mathbf{f}(n) \in \mathcal{O}_S$ of the power sum $\mathbf{f}$ generates the ideal $(g^n)^*(D)$, where $D$ is viewed as a divisor in $\mathbb{G}_m^r$, so its pull-back $(g^n)^*(D)$ is an ideal of $\mathcal{O}_S$. Now, let us consider two power sums $\mathbf{f}_1, \mathbf{f}_2$ with values in a ring of $S$-integers; they correspond to two $S$-integral points $g_i$ in tori $\mathbb{G}_i$ and divisors $D_i$, for $i = 1, 2$. The condition that $\mathbf{f}_1(n)$ divides $\mathbf{f}_2(n)$ for some value of $n$ can be expressed in terms of inclusions of corresponding ideals. The conclusion of Theorem 4 that $\mathbf{f}_1$ divides $\mathbf{f}_2$ in the ring of power sums can be translated, at least under suitable technical hypothesis, by saying that a suitable isogeny takes $D_1$ to $D_2$. Precisely, in [4] Noguchi and the author derived from the main results of [6] the following statement:

**Theorem 7** *Let $\mathcal{O}_S$ be a ring of $S$-integers in a number field $k$. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be linear tori, and let $g_i \in \mathbb{G}_i(\mathcal{O}_S)$ be elements generating Zariski-dense subgroups in $\mathbb{G}_i$ $(i = 1, 2)$. Let $D_i$ be irreducible divisors defined over $k$ with trivial stabilizer. Suppose that for infinitely many natural numbers $n$, the inclusion of ideals*

$$(g_1^n)^*(D_1) \supset (g_2^n)^*(D_2) \tag{1}$$

*holds. Then there exists an étale morphism $\phi : \mathbb{G}_1 \to \mathbb{G}_2$, defined over $k$, and a positive integer $h$ such that $\phi(g_1^h) = g_2^h$ and $D_1 \subset \phi^*(D_2)$.*

The condition on the stabilizer of the divisors $D_i$ can be relaxed, but cannot be completely avoided. For instance, take $k = \mathbb{Q}$, $\mathcal{O}_S = \mathbb{Z}$, $\mathbb{G}_1 = \mathbb{G}_m$, $D_1 = \{1\}$; then $\mathbb{G}_2 = \mathbb{G}_m^2$, $D_2 = \{1\} \times \mathbb{G}_m + \mathbb{G}_m \times \{1\}$, so that $D_2 = F^{-1}(0)$ for the polynomial $F(X_1, X_2) = (X_1 - 1)(X_2 - 1)$. Choose $g_1 = 2, g_2 = (2, 3)$. Clearly condition 1 is satisfied for every $n$, as it amounts to the fact that $2^n - 1$ divides $(2^n - 1)(3^n - 1)$, but there exists no dominant map $\mathbb{G}_1 \to \mathbb{G}_2$.

The above formulation leads naturally to generalizations, both in the arithmetic and in the analytic setting. Still remaining in the arithmetic realm, one is tempted to replace tori by abelian or semi-abelian varieties. We leave this as a conjecture, since the techniques of [6] do not seem to apply easily to the compact case. A related conjecture by Silverman, formulated in [11], attempts to extend Theorem 2 to elliptic curves. It states the following:

Given an elliptic curve $E$ defined over $\mathbb{Q}$ via a Weierstrass model, for a point $P \in E(\mathbb{Q})$ write $x(P) = A(P)/D(P)$ as a fraction in lower terms. Take two independent points $P, Q \in E(Q)$. Then $\log \gcd(D(nP), D(nQ))$ should be $o(n^2)$.

The above conjecture, which constitues the compact analogue of Theorem 2, would follow from the celebrated Vojta's conjectures, as explained by Silverman [11].

In another direction, one could ask for the same conclusion of Theorem 7 under the hypothesis of the inclusion of the *supports* of the divisors $(g_i^n)^*(D_i)$. For this problem some special result has been obtained by Barsky, Bézivin and Schinzel, but, as already mentioned, even in the one dimensional case the general problem remains open.

For the analytic analogue, which holds in the general case of semi-abelian varieties, we refer the reader to Noguchi's contribution. For instance, the gcd estimates of Theorem 2 admit a Nevanlinna theoretic analogue, proved by Noguchi-Winkelmann-Yamanoi, which also holds for elliptic curves; so the analytic analogue of Silverman's conjecture is proved in Nevanlinna's theory.

It is worth to notice that the corresponding statement in Nevanlinna theory to Theorem 7, which, as we said, holds in general for holomorphic maps to semi-abelian varieties, is phrased in exactly the analogue way, via the well-known correspondence between arithmetic geometry and Nevanlinna theory; especially its conclusion is just the same.

## References


[1] Ailon, N., Rudnick, Z., Torsion points on curves and common divisors of $a^k - 1, b^k - 1$, Acta Arith. 113, 2004, 31-38.

[2] Bugeaud, Y., Corvaja, P., Zannier, U., An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, Math. Zeit. **243** (2003), 79-84.

[3] Corrales-Rodrigáñez, C. and Schoof, R., The support problem and its elliptic analogue, J. Number Theory **64** (1997), 276-290.

[4] Corvaja, P. and Noguchi, J., A New Unicity Theorem and Erös' Problem for Polarized Semi-Abelian Varieties, preprint 2009.

[5] Corvaja, P. and Zannier, U., Diophantine equations with power sums and universal Hilbert sets, Indag. Math. **N.S. 9(3)** (1998), 317-332.

[6] Corvaja, P. and Zannier, U., Finiteness of integral values for the ratio of two linear recurrences, Invent. Math. **149** (2002), 431-451.

[7] Corvaja, P. and Zannier, U., Lower bound for the height of a rational function at $S$-unit points, Monatsh. Math. **144** (2005), 203-224.

[8] Larsen, M., The support problem for abelian varieties, J. Number Th. **101** (2003), 398-403.

[9] van der Poorten, A. J., Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, C. R. Acad. Sci. Sér. I Math. **306** (1988), 97–102.

[10] Schinzel, A., On the congruence $a^x \equiv b \pmod{p}$, Bull. Acad. Polon. Sci. **8** (1960), 307-309; Selecta Vol. 2, 909-911, EMS 2007.

[11] Silverman, J., Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups, Monatsh. Math. (4) 145 (2005), 333-350.



Dipartimento di Matematica e Informatica
Università di Udine
Via delle Scienze, 206 - 33100 Udine
e-mail: pietro.corvaja@dimi.uniud.it